Tutorial Questions: Unit 2- Introduction to Classical Cryptography

Perform the following exercises after reading the lecture resource Unit 2 – Introduction to Classical Cryptography. Assume plaintexts and ciphertexts are English words and phrases. You may wish to write Java or Python programs to help you solve the problems.

Exercise 1

Given that the following ciphertext was encrypted using Caesar Cipher:

`VYBIRPELCGBTENCUL`

It is known that the first plaintext character is `'i'`, find the plaintext message.

Exercise 2

Decrypt each of the following Caesar encryptions...

(a) `WKHRQOBFRQVWDQWLQOLIHLVFKDQJH`
(b) `YMJXJHWJYTKLJYYNSLFMJFINXLJYYNSLXYFWYJI`
(c) `JOHUNLFVBYAOVBNOAZHUKFVBJOHUNLFVBYDVYSK`

Exercise 3

For this exercise, use the simple substitution table given in Table below.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
N	O	Q	F	B	W	H	G	P	R	L	I	A	V	D	S	E	K	U	Z	Y	X	J	T	C	M

Table 1: Simple substitution encryption table

(i) Encrypt the plaintext message

`You have not failed until you quit`

(ii) Make a decryption table, that is, make a table in which the ciphertext alphabet is in order from A to Z and the plaintext alphabet is mixed up.

(iii) Use your decryption table from (b) to decrypt the following message.

`DVQBJ BNQQB SZDYK IPAPZ UJBHD OBCDV FZGBA`

Exercise 4

A *transposition cipher* is a cipher in which the letters of the plaintext remain the same, but their order is rearranged. ...

(a) Use this transposition cipher with key = 5 to encrypt the letters of the following message, after all punctuation and special characters are removed:

`I never dreamed about success. I worked for it`

(b) The following message was encrypted using this transposition cipher with key = 5. Decrypt it.

`EGWON OXBCE ASTRE HYNEH LHNUT IWXTA OTEED`

Exercise 5

Encrypt each of the following Vigenère plaintexts using the given keyword:

(a) Keyword: `hamlet`
Plaintext: `To be, or not to be, that is the question.`
(b) Keyword: `fortune`
Plaintext: `The treasure is buried under the big tree.`

Exercise 6

Decrypt the following Vigenère ciphertext using the keyword power:

`SSISTGOYC`

Exercise 7

Encrypt each of the following plaintext using the autokey cipher with the given keyword best:

`NEKVMRWKGEIA`

Exercise 8

(a) Encrypt the following plaintext using the **Playfair** method and keyword `cryptography` :

Plaintext : `Law of Lords`

(b) Decrypt the following ciphertext using the **Playfair** method and keyword `godzilla`:

Ciphertext : `NICTGHQNNYGOBT`